referenced patent application, 09/844,439 OCL-1, "Method and System for Establishing a Remote Connection To a Personal Security Device." An additional limitation of this method becomes apparent when attempting to perform multiple authenticating transactions using a single PSD over a network connection. The PSD, beings a slow serial device, only allows one transaction to occur at a time. In addition, network contention and processor execution speed issues become particularly problematic when low bandwidth connections (e.g. dialup connections) are made between a client and a remote computer system during authentication with the PSD.

Summary of Invention

This invention resides in a method of authenticating an end user to one or more remote computer systems using a communications pipe to send authentication codes from a PSD to one or more secure remote computer systems. The remote computer system establishing and maintaining the communications pipe with the PSD performs an initial authentication, then acts as a secure hub and client authentication proxy for other remote computer systems requesting client authentication. In a multi-tasking operating environment, multiple authentications occur as background transactions, which are transparent to the end user. The remote computer system acting as a secure hub may form multiple communications pipes with other clients connected to a network.

In order to perform authentications, a communications pipe is established between a remote computer system and a PSD as previously described in cross-referenced patent application, 09/844,439 OCL-1, "Method and System for Establishing a Remote Connection To a Personal Security Device." A remote computer system requiring client authentication sends an authentication challenge to either the client and is redirected to the remote computer system acting as a secure hub or using a pre-established address, sends an authentication challenge directly to the remote computer system maintaining the communications pipe.

In a one embodiment of this invention, the remote computer system assigned as a secure hub performs the initial client authentication then routes subsequent authentication challenges through the communications pipe to the PSD for processing within the secure domain of the PSD, then returns the PSD generated authentication code back through the communications pipe over a network and to the challenging remote computer system.

In a second embodiment of this invention, the remote computer system established as a secure hub performs the initial client authentication then copies, if not already present, the PSD's authentication credentials through the communications pipe to a secure storage location within the secure hub. The secure hub using the transferred

PSD credentials and equivalent algorithms authenticates the client to subsequent remote computer systems by emulating the PSD.

In both embodiments of this invention, communications between local clients and remote computers systems over one or more networks should employ secure communications protocols as is described in the cross-referenced patent application, 09/844439 OCL-1, which further reduces the likelihood of unauthorized access or interception. For non-proprietary transactions with the PSD, secure communications are optional.

There are several advantages to this invention when used in conjunction with the communications pipe. First and most importantly, authentication transactions are only performed in highly secure and protected domains, which greatly reduces the chances of unauthorized access or interception. Secondly, authentication transactions will occur more rapidly and seamlessly, since remote computer systems are generally provided with greater network bandwidth and processing power than local clients.

Lastly, by relocating the authentication process to a remote computer system, a more simplified means to perform end-to-end authentication and maintain an audit trail of transactions by authenticated end users and transactions with other remote computer systems is readily accomplished since all authentication transactions are routed through a remote computer system designated as a secure hub.

Additional security improvements may be facilitated by incorporating the use of hardware security modules (HSM) at designated remote computer systems implementing the secure hub portion of the invention. End-to-end security is enhanced since authentications and related transactions occur within the highly secure domains of a PSD and HSM.

Please Enter dtg 03/02/07

## Brief Description of Drawings

FIG. 1 - is a general system block diagram for implementing present invention.

FIG. 2 - is a detailed block diagram illustrating initial authentication challenge.

FIG. 3 - is a detailed block diagram illustrating initial authentication.

FIG. 4 - is a detailed block diagram illustrating remote authentication challenge.

FIG. 5 - is a detailed block diagram illustrating remote authentication.

FIG. 6 - is a detailed block diagram illustrating authentication credential transfer.

FIG. 7 - is a detailed block diagram illustrating remote authentication challenge (Alternate inventive embodiment.)

Replacement Sheet



FIG. 8 - is a detailed block diagram illustrating remote authentication (Alternate inventive embodiment.)

Detailed Description of Preferred Embodiment

The steps involved in performing authentication through a communications pipe are shown in Figures 1 through 8. Figure 1 is a generalized system block diagram. Figures 2 through 5 illustrate one embodiment of the invention where responses to authentication challenges are generated within the secure domain of a Personal Security Device. Figures 6 through 8 illustrate a second embodiment of the invention where a remote computer system established as a secure hub provides the proper response to authentication challenges, rather than directing challenges through the communications pipe into the PSD for processing. Characters shown with a prime sign (e.g. C') indicate a duplicate of an original authentication credential. Other drawing details shown but not described in this application refer to information described in cross-referenced patent application, 09/844,439 OCL-1, "Method and System for Establishing a Remote Connection to a Personal Security Device."

Referring now to FIG. 1, a generalized system block diagram of the invention where Client 10 and a connected Personal Security Device 40 is connected over a network 45 with a remote computer system 50 using a communications pipe 75 as described in co-pending patent application 09/844,439 OCL-1. A remote computer system 50, is operating as a secure hub following initial authentication as described below, to service authentication requests made by other remote computer systems sent over a network 45 or 45A.

The remote computer system 150 is an example of a system requiring authentication when a request for secure functions or data is sent from client computer 10 over the networks 45 and 45A. The communications pipe 75 applies to authentication transactions but does not restrict nor control non-secure transactions occurring over either network 45 or 45A.

Networks 45 and 45A may be a common network as in a virtual private networking arrangement or separate networks such as private intranet and public internet arrangements. The networks 45 and 45A are depicted separately for illustrative purposes only. No limitation is intended in the number of PSDs and clients forming communications pipes 75 with one or more secure hubs 50; nor should any limitation on the number of remote computer systems 70 available for authentication be construed from the drawing. Transactions not involving authentications are not restricted to the secure hub.

Please Enter 03/02/07

Replacement Sheet